正則集合に表現等価なテンポラル・ロジック(アルゴリズムの数学的基礎理論とその応用)

AUTHOR(S):

平石, 裕実; 矢島, 脩三

CITATION:

平石, 裕実 ...[et al]. 正則集合に表現等価なテンポラル・ロジック(アルゴリズムの数学的基礎理論とその応用). 数理解析研究所講究録 1986, 591: 268-277

ISSUE DATE:

1986-05

URL:

http://hdl.handle.net/2433/99456

数理解析研究所講究録
591巻 1986年 268-277

正則集合に表現等価なテンポラル・ロジック

京大工学部　平石裕実（Hiromi Hiraishi）
京大工学部　矢島脩三（Shuzo Yajima）

1．まえがき

超大規模論理回路（VLSI）により大規模論理システムの構築が可能となりつつある現在、大規模論理システムを誤りなく正しく設計し、かつ実現して正しく動作していることの確認できる論理設計手法の確立が益々重要となってきている。このため、従来より論理設計のCAD/DA、論理設計手法、故障検査、設計検証等の研究が行われているが、論理設計検証については未だ実用的な手法が確立されておらず、設計対象システムの形式的仕様記述や形式的検証手法の研究が重要と考えられる。

形式的仕様記述や形式的検証のアプローチとしては、命題論理や第1階述語論理、テンポラル・ロジック[1]等の論理体系に基づく方法や、VDM[2]や抽象データ型[3]による仕様記述等の代数的方法、また、正則集合や第1#表現[4]等の系列記

述に基づく方法等がある。特にテンポラル・ロジックは時間の概念を陽に表現できるため、現在、並行プロセスやハードウェアの設計検証との関連で研究が進められており、種々のクラスのテンポラル・ロジックが提案されている。拡張テンポラル・ロジック（ＥＴＬ）[5]は無限長系列を取り扱いω-正則集合を表現できるが、そのためには無限個のテンポラル演算子を必要とする。一方、インターバル・テンポラル・ロジック（ＩＴＬ）[6]は有限長系列を取り扱い、その表現能力は真に正則集合を含んでいるが、充足可能性判定問題が決定不能になる等の問題点を含んでいる。設計対象を有限オートマトンと考えると、正則集合と表現能力が等価なテンポラル・ロジックの体系を明らかにすることが重要であると考えられる。そこで本稿ではこのような観点から正則集合と等価な表現能力を持つ新たなテンポラル・ロジック（ＲＴＬ）を示す。

２．ＲＴＬ

２．１　ＲＴＬのシンタックス

【定義１】　ＲＴＬの原始記号

以下に述べる原始命題、論理記号、補助記号をＲＴＬの原始記号という。

（１）原始命題　ｐ，ｑ，ｒ，・・・

（２）論理記号　～，∨，○，⊡，：

（３）補助記号　（，）　□

原始命題の集合を以下ＡＰで表わす。

【定義２】　ＲＴＬの論理式（ＲＴＬ式）

（１）ｐが原始命題の時，ｐはＲＴＬ式である。

（２）ηがＲＴＬ式の時、（～η）もＲＴＬ式である。

（３）η，ξがＲＴＬ式の時、（$\eta \vee \xi$）もＲＴＬ式である。

（４）ηがＲＴＬ式の時、（○η）もＲＴＬ式である。

（５）ηがＲＴＬ式の時、（⊡η）もＲＴＬ式である。

（６）η，ξがＲＴＬ式の時、（η：ξ）もＲＴＬ式である。

（７）以上の（１）－（６）を有限回適用して得られるもののみがＲＴＬ式である。　□

ＲＴＬ式全体の集合をＬＦで表わす。又、論理記号～，○，⊡は∨，：よりも高い優先順位を持つものとし、論理記号の適用範囲が明確な場合は補助記号（，）を省略することがある。更に、次の略記を適宜用いる。

$\eta \wedge \xi \triangleq \sim(\sim\eta \vee \sim\xi)$，$\eta \supset \xi \triangleq \sim\eta \vee \xi$，$\eta \equiv \xi \triangleq (\eta \supset \xi) \wedge (\xi \supset \eta)$，$\Diamond\eta \triangleq \sim\boxdot\sim\eta$，$V_f \triangleq \eta \vee \sim\eta$，

$U_f \triangleq \sim V_f$ 。

２．２　ＲＴＬのセマンティックス

【定義３】　ＲＴＬの解釈

Σを状態の有限集合、Ｂ＝｛Ｔ，Ｆ｝を真理値の集合とし、各状態ｓにおける原始命題ｐの真理値を与える関数 m_s：Σ×ＡＰ→Ｂと、状態の空系列を表わすλに対する原始命題ｐの真理値を与える関数 m_λ：ＡＰ→Ｂを考える。この時、$<\Sigma, m_s, m_\lambda>$をＲＴＬの解釈という。　□

【定義４】　ＲＴＬ式の真理値

Σ上の系列 $\sigma \in \Sigma^*$（$\sigma = \lambda$ 又は $\sigma = s_0 s_1 \cdots s_n$とする）に対してＲＴＬ式の真理値を与える関数Ｍ：$\Sigma^* \times LF \rightarrow$Ｂを次のように定義する。但し、

$p \in AP$，$\eta, \xi \in LF$とし、$|\sigma|$は系列σの長さを表わし、$|\sigma| \geq 2$の時 $\sigma_1 = s_1 s_2 \cdots s_n$、$|\sigma| = 1$の時 $\sigma_1 = \lambda$とする。

（１）$M(\sigma, p) = m_s(s_0, p)$ ‥‥　$|\sigma| \geq 1$の時

$m_\lambda(p)$　‥‥　$\sigma = \lambda$の時

（２）$M(\sigma, \sim\eta) = T$ ‥‥ $M(\sigma, \eta) = F$の時

F ‥‥ $M(\sigma, \eta) = T$の時

（３）$M(\sigma, \eta \vee \xi) = T$ ‥‥ $M(\sigma, \eta) = T$

または $M(\sigma, \xi) = T$ の時

F ‥‥ それ以外の時

（４）$M(\sigma, \bigcirc \eta) = T$ ‥‥ $\sigma = \lambda$ で $M(\lambda, \eta) = T$

または $\sigma \neq \lambda$ で $M(\sigma_1, \eta) = T$ の時

F ‥‥ それ以外の時

（５）$M(\sigma, \boxdot \eta) = T$ ‥‥ $M(\alpha_i, \eta) = T$ なる

$\alpha_i \in \Sigma^*$（$1 \leqq i \leqq m \leqq n$）が存在して、

$\sigma = \alpha_1 \alpha_2 \cdot\cdot\cdot \alpha_m$ と表わせる時

F ‥‥ それ以外の時

（６）$M(\sigma, \eta : \xi) = T$ ‥‥ $M(\alpha_1, \eta) = T$，

$M(\alpha_2, \xi) = T$ なる $\alpha_i \in \Sigma^*$（$i = 1, 2$）

が存在して、$\sigma = \alpha_1 \alpha_2$ と表わせる時

F ‥‥ それ以外の時　□

$M(\sigma, \eta) = T$ の時、$< m_s, m_l, \sigma > \vDash \eta$ と表わし、m_s, m_l が明確な場合は単に $\sigma \vDash \eta$ と表わす。　又、任意の m_s, m_l, σ に対して $< m_s, m_l, \sigma > \vDash \eta$ の時、η は恒真であるといい $\vDash \eta$ と表わす。

３．ＲＴＬの表現能力

解釈 $< \Sigma, m_s, m_l >$ のもとでＲＴＬ式 η の真理値をＴと

するようなΣ上の系列全体の集合を$L<\Sigma, m_s, m_l>(\eta)$とする。即ち、

$L<\Sigma, m_s, m_l>(\eta) = \{\sigma \mid \sigma \in \Sigma^*, <m_s, m_l, \sigma> \models \eta\}$

この時、ηは$L<\Sigma, m_s, m_l>(\eta)$を表わすという。以下、混乱の恐れがない時は$L<\Sigma, m_s, m_l>(\eta)$を単に$L(\eta)$と表わす。

RTLの表現能力に関して以下の補題が成立する。

【補題1】 $L(\eta)$はΣ上の正則集合である。

（略証） RTL式の構成方法に基づく帰納法により示す。

（1） $p \in AP$, $S(p) = \{s \mid s \in \Sigma, m_s(s, p) = T\}$とすると、

$m_l(p) = T$ならば、$L(p) = \lambda + S(p) \cdot \Sigma^*$

$m_l(p) = F$ならば、$L(p) = S(p) \cdot \Sigma^*$

（2） $L(\sim\eta) = \Sigma^* - L(\eta)$

（3） $L(\eta \vee \xi) = L(\eta) + L(\xi)$

（4） $L(\bigcirc\eta) = \lambda + \Sigma \cdot L(\eta)$ $\lambda \in L(\eta)$の時

$\Sigma \cdot L(\eta)$ ‥‥ $\lambda \notin L(\eta)$の時

（5） $L(\boxdot\eta) = L(\eta)^+$

（6） $L(\eta : \xi) = L(\eta) \cdot L(\xi)$ □

【補題２】　Σ上の任意の正則集合Rに対し、ある解釈＜Σ，m_s，m_1＞のもとでRを表わすＲＴＬ式ηが存在する。

（略証）　「$\log_2|\Sigma|\rceil + 1$個の原始命題p_0，p_1，・・・・，$p_{\log_2|\Sigma|}$を用い、m_1，m_sを次のように決める。

		p_0	p_1	p_2	・・・・	$p_{\log_2\|\Sigma\|}$	
m_1	λ	T	F	F	・・・・	F	F
	s_1	F	F	F	・・・・	F	F
	s_2	F	F	F	・・・・	F	T
m_s	s_3	F	F	F	・・・・	T	F
	・	・	・	・	・・・・	・	・
	・	・	・	・	・・・・	・	・
	$s_{\|\Sigma\|}$	F	T	T	・・・・	・	・

即ち、s_iに対して真となる$p_1' \wedge p_2' \wedge \cdots \wedge p_{\log_2|\Sigma|}'$の形の論理式は一意的に定まり、異なる$s_i$と$s_j$に対しては異なる論理式が対応する（但し、$p_k'$は$p_k$あるいは$\sim p_k$を表わす）。又、$p_0$はλに対してのみ真となる原始命題である。

この時、正則集合Rを表わすＲＴＬ式をＲＴＬ（Ｒ）とすると、ＲＴＬ（Ｒ）は下記のように再帰的に構成できる。但し、R_1，R_2はΣ上の任意の正則集合とする。

ＲＴＬ（ϕ）＝　U_f

$RTL(\lambda) = p_0$

$RTL(s_1) = \sim p_1 \wedge \sim p_2 \wedge \cdots \wedge \sim p_{\lfloor \log_2 |\Sigma| \rfloor} \wedge \bigcirc p_0 \wedge \sim p_0$

$RTL(R_1 \cdot R_2) = (RTL(R_1)) : (RTL(R_2))$

$RTL(R_1 + R_2) = (RTL(R_1)) \vee (RTL(R_2))$

$RTL(R_1^*) = p_0 \vee \Box (RTL(R_1)) \quad \Box$

これより次の定理が成立する。

【定理１】 ＲＴＬは正則集合と等価な表現能力を持つ。□

４．ＲＴＬ式の恒真性判定問題

ＲＴＬ式の恒真性判定について以下の定理が成立する。

【定理２】 与えられたＲＴＬ式ηが恒真かどうかの判定問題は決定可能である。

（略証） まず、m_1，m_sを固定して考える。この時、ηが表わす系列集合を正則表現Ｒで表現すると、任意の$\sigma \in \Sigma^*$に対して$< m_s, m_1, \sigma > \models \eta$かどうかの判定問題はＲの空補集合判定問題に帰着できるので決定可能である。

次に、任意のm_1，m_sについて考える。m_1はＡＰ→Ｂなる

関数で、m_sは$\Sigma \times AP \rightarrow B$なる関数であるが、$\eta$の長さは有限であり高々有限個の原始命題しか含んでいない。ηに含まれていない原始命題の各状態に対するT／Fの値はηの真理値に影響を与えないので、ηに含まれる有限個の原始命題に対するT／Fの割り当てのみを考えれば十分である。又、Σは有限集合であるので、m_1, m_sとしては高々有限個の関数のみを考えればよい。

以上により、ηが恒真かどうかの判定問題は決定可能である。 □

【定理３】 RTL式の恒真性判定問題のDTM領域複雑度は非初等的である。

（略証） RTL式と拡張正則表現との間の変換は多項式時間で可能であり、拡張正則表現の空集合問題のDTM領域複雑度は非初等的である[7]ことより明らか。 □

５．あとがき

正則集合と等価な表現能力を持つテンポラル・ロジックRTLを導入し、その恒真性判定問題が決定可能でありDTM領域複雑度がであることを示した。今後RTLの公理系を明らかにすると共に、論理設計検証への応用を考えていきたい。

謝辞　種々御議論頂いた矢島研究室の諸氏に感謝します。

参考文献

[1] N.Rescher and A.Urquhart：Temporal Logic, Springer-Verlag, 1971.

[2] D.Bjorner：Formal Specification & Software Development.

[3] 稲垣，坂部：抽象データタイプの代数的仕様記述の基礎(1)(2)，情報処理，vol.25, no.1, pp.47-53, no.5, pp.491-501, 1984.

[4] 木村，矢島：論理回路の入力制約および入出力仕様の記述とその検証，信学技報，AL85-65, 1986.

[5] P.Wolper：Temporal Logic Can Be More Expressive, Proc. 22nd Annual Symp. on Foundations of Computer Science, pp.340-348, 1981.

[6] B.Moszkowski：Reasoning about Digital Circuit, STAN-CS-83-970, 1983.

[7] A.V.Aho, J.E.Hopcroft and J.D.Ullman：The Design and Analysis of Computer Algorithms, Adison-Wesely, 1974.